Australian Ministerial Roundtable: Facebook opening remarks (written version)

Mia Garlick, Director of Public Policy, Australia and New Zealand
I would like to start by sharing my deepest sympathies to the people, families and communities affected by the recent attacks in New Zealand – particularly to you High Commissioner.

We are all in agreement that not only should these attacks never have occurred, but also they should never have been able to be livestreamed in this way and then reshared as widely as they were.

I want to emphasize that this content absolutely violates our policies and we understand that we have a responsibility to work with government and regulators to try to stop bad actors from co-ordinating the misuse of our services in this way again.

From our review of what happened so far, we believe that working with you to develop an effective response here has three components:

1. Security – my colleague Nathaniel Gleicher, our Director of Cybersecurity globally is best placed to speak to this
2. Extremism – my colleague Gullnaz Baig who leads our counter-terrorism and counter-extremism work in APAC is best placed to speak to this
3. Law Enforcement – my colleague Jeff Wu who leads our law enforcement liaison in APAC and has had a member his team on the ground working with New Zealand Police is best placed to speak to this

Out of respect for the seriousness of this issue and your leadership Prime Minister, my colleagues have flown to be here today to participate directly in this conversation with you as we review lessons learned and the solutions that we can work on together to protect Australians.

Nathaniel Gleicher, Director of Cybersecurity Policy

Thanks Mia. Let me say a bit about what happened on our platforms, and what we're doing to make these tactics more difficult in the future.

Let's start with a few key details. We know the video was viewed fewer than 200 times during the live broadcast, and including the views during the live broadcast, the video was viewed about 4000 times in total before being removed from Facebook. In the first 24 hours, we removed about 1.5 million videos of the attack globally. More than 1.2 million of those videos were blocked at upload, and were therefore prevented from being seen on our services.

In other words, the vast majority of this video's spread came from people re-editing and re-sharing the video *after* its initial broadcast, which means that to tackle this challenge, we must focus not just on recording services, but on video uploads and re-uploads.

In understanding those re-uploads, we know that a core community of determined bad actors actively worked to not only rebroadcast this video, but continually re-edit the video to make it more difficult for automated systems to block. We also know that a number of media outlets broadcast their own segments of the video. Covering these types of deadly acts is important because it educates the public, but showing the video itself unfortunately provides those bad actors with additional material for their efforts. Rather than simply dealing with many copies of the same video, we have already identified and blocked more than a thousand distinct videos depicting some part of those terrible 17 minutes.

These factors demonstrate that this is an adversarial problem. By this I mean that the bad actors we face will work to defeat any security protocols we put in place. When dealing with a challenge like this, we can't rely on any *single* security approach, because we have to continually work to stay ahead.

Instead, we are layering together a series of controls, including (1) improving our automated detection; (2) prioritizing and accelerating user reporting; and (3) finding and disrupting the communities on 8chan and elsewhere where this coordination is happening.

We know that bad actors like this will keep trying. But by combining our efforts with our partners here in industry and government, we can make these tactics much more difficult. And that's our highest priority.

Let me hand over to my colleague, Gullnaz Baig, to talk about how this effort fits into our broader response to extremism.

Gullnaz Baig, Head of Public Policy, Counterterrorism and Dangerous Organizations, Asia-Pacific

Thanks Nathaniel. Beyond the security considerations, let me share how we tackle the broader issue of extremism and terrorism on Facebook. Our position is simple - terrorism, extremism or graphic violence have no place on Facebook, and we have clear rules against each of these.

Immediately following the New Zealand attack, we designated this a terror attack, meaning that any praise, support, or representation violates our Community Standards and is not permitted on Facebook. Given the severe nature of the video, we also prohibited its distribution even if shared to raise awareness, or only a segment shared as part of a news report. And we removed the personal accounts of the named suspect from Facebook and Instagram, and are actively identifying and removing any imposter accounts that surface.

Our approach to tackling extremism and terrorism on our services has evolved over time as we learn from our community, from experts in the field, and as technology provides us new tools to operate more quickly, more accurately and more precisely at scale. We use a combination of people and technology to identify and remove content and accounts that violate our policies, and over time we have got better at detecting it before people even see it. For example, between July and September last year we removed 99.5% of terrorist content before it was reported to us. And our proactive rate for graphic violent content increased more than 25 percentage points in the last year, and is now more than 97 percent.

Over the years we've also significantly grown our team of counterterrorism and extremism specialists. Approximately 200 people are exclusively or primarily focused on countering terrorism as their core responsibility. This includes academic experts on counterterrorism, former prosecutors, former law enforcement agents and analysts, and engineers. I am part of this team, and it is part of my to help identify and remove extremist organizations who violate our policies. This includes white supremacists. We currently enforce against more than 200 white supremacist organizations globally. In late 2018, we banned Blair Cotrell and removed the United Patriots Front Facebook Page for hate speech violations. This morning we have banned Neil Erikson, Tom Sewell, the Lads Society, the United Patriots Front and the Antipodean Resistance from Facebook and Instagram, for violating our dangerous individuals and organizations policy. This means they will no longer be allowed a presence on our services, and we will also remove praise and support of these individuals and groups when we become aware of it. We don't want people or organizations who spread hate to find a platform on our services, and we will continue to review and assess those who engage in this kind of offline behaviour.

Working to keep terrorism and extremism off Facebook isn't enough because terrorists and extremists can jump from platform to platform. That's why partnerships with others – including other companies, civil society, researchers and governments – are so crucial. One example of this is the Global Internet Forum to Counter Terrorism (GIFCT).

Members of the Global Internet Forum to Counter Terrorism (GIFCT) coordinate regularly on terrorism and have been in close contact since the terrorist attack in New Zealand. We have shared digital fingerprints of more than 100,000 visually distinct images, and more than 1,000 visually-distinct videos related to the attack via our collective database, along with URLs and context on our enforcement approaches. This incident highlights the importance of industry

cooperation regarding the range of terrorists and violent extremists operating online. We are experimenting with sharing URLs systematically rather than just content hashes, are working to address the range of terrorists and violent extremists operating online, and intend to refine and improve our ability to collaborate in a crisis.

Our collaboration with law enforcement is also an important component to tackling terrorism and extremism, Let me hand over to my colleague Jeff Wu, who leads our law enforcement team in the region to talk more about this.

Jeff Wu, Director of Law Enforcement, Asia-Pacific
Thanks Gullnaz. Allow me to share a bit about our interactions with law enforcement and what we're doing to support them the long-term.

Facebook has a global Law Enforcement Outreach team dedicated to working with law enforcement and security agencies. Our job is to engage in strategic relationships and initiatives with first responders, law enforcement and security agencies that strengthen coordination between Facebook and the Government. Collectively, the team consists of former law enforcement agents, federal prosecutors, military and intelligence officers and cyber security experts.

Specifically, for the New Zealand attack, we have been working directly with the New Zealand Police to respond to the attack and to support their investigation. In the immediate aftermath of the attack, a member of my team was dispatched to Wellington to be the on-the-ground Facebook resource for law enforcement authorities. My team assisted New Zealand Police in coordinating the legal requests for user data information, expedited content removal reports and helped police navigate Facebook's policy and procedures to minimize any procedural or legal delays.

Second, our team has also been in Australia for the past week, meeting with existing Law Enforcement and Security contacts across various agencies, including the Australian Federal Police, ASIO and equivalent departments within the Queensland Police. Our work in Australia continues with a visit to Sydney planned for the remainder of this week. We are committed to working with authorities to help keep their communities safe.

Our greatest priorities right now are to support the New Zealand Police in every way we can, and to continue to understand how our systems and other online platforms were used as part of these events so that we can identify the most effective policy and technical steps.

What happened in New Zealand is horrific. Our hearts are with the victims, families and communities affected by this horrible attack. There is no place on Facebook for terrorism and extremism, and we share your goal of stopping terrorists and extremists from using social media. We appreciate the opportunity to be here today to discuss our actions following these attacks and our ongoing work to protect the safety and integrity of our services. Thank you.